CLAIMS

1. A method for preventing an administrator to impersonate a user of a relational database, which database at least comprises one table with at least one user password, which password is used for logging on to said database, wherein said password is stored as a hash value, said method comprising the steps of:

adding a trigger to said table, said trigger at least triggering an action when an administrator alters said table through a database management system (DBMS) for said database;

calculating a new password hash value differing from said stored password hash value when said trigger is triggered; and

replacing said stored password hash value with said new password hash value.

2. A method according to claim 1, comprising the further steps of:

calculating a check value of said trigger, such as a hash value; and

comparing said trigger control value at the startup and at regular intervals with a recalculated check value.

3. A method according to claim 1 or 2, comprising the further step of comparing for each active user having access to sensitive data, the hash value of the current login password with the hash value of the currently stored password.

4. A method according to claim 3, wherein the further step of comparing is performed after every change of the database content by said user.

5. A method according to claim 1 or 2, wherein said trigger comprises means for reading a log of actions on said database, means for identifying commands for altering user passwords in said log and means for identifying which user passwords that have been changed.

6. A relational database system for preventing an administrator impersonating another user, which database at least comprises one table with at least one user password, wherein said password is stored as a hash value, said system comprising:

calculation means for calculating a hash value of a user password, which calculation means is not accessible by said administrator;

trigger means, which trigger at least said calculation means for calculation of a new hash value of said password when an administrator alters said table through a database management system (DBMS) of said database; and

replacing means for replacing said stored hash value with said new hash value for each triggered calculation.